-----Original Message-----
From: Tom Cross
Sent: Monday, October 26, 2015 2:41 PM
To: Aaron Amundson
Cc: Jonathan Wise
Subject: Re: ISTAC meeting October 28th - Discussion of the Definition of "Intrusion Software"

Aaron, Jonathan,

Unfortunately I have a confict on October 28th, but I wanted to provide a written statement, which follows:

Dual-Use Export Controls are designed to prevent the proliferation of technology. The intent is not only to prevent weapons from falling into the wrong hands, but also knowledge of how to build, maintain, and use weapons. In computer security, the technical knowledge that defenders need in order to protect infrastructure from attack is exactly the same knowledge that attackers require, and often the same tools that attackers use are used to test defenses. Because of this, a non-proliferation approach can be counter productive. It is very difficult to describe these tools and technologies in a way that clearly differentiates things are are useful for offensive purposes from things that defenders need. For these reasons, a general anti-proliferation approach will have a negative impact on the security of the Internet.

It seems reasonable that the United States might want to prohibit American companies from directly providing offensive information security tools and technology to governments of States who use those tools in ways that we find objectionable. A more narrow way to achieve that would be to control transactions where the technology is an offensive computer security tool that is specially designed for gaining unauthorized access to computer systems or networks, AND the customer is a government or military end user, or where the seller has reason to know that the technology will be diverted to a government or military end user. It would also help to further narrow the list of prohibited customers to small list of specific governments or militaries that are a concern, so that general coordination of information about computer security issues with most foreign governments is not impacted.

By coupling the technology control with a narrow list of prohibited customers, some human rights objectives can be achieved without a widespread negative impact on global coordination about information security issues. This suggested approach may not be consistent with the structure of the Wassenaar Arrangement and may be better implemented through other legal mechanisms.

Regards,
Tom Cross
CTO - Drawbridge Networks